

#2
2-502
gm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of : **Hiroyuki SUZUKI**
Filed: : **Concurrently herewith**
For: : **SYSTEM PROVIDING A VIRTUAL....**
Serial No. : **Concurrently herewith**

JC973 U.S. PTO
09/998550
11/29/01

Assistant Commissioner for Patents
Washington, D.C. 20231

November 29, 2001

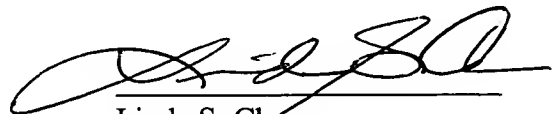
PRIORITY CLAIM AND
SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-253308** filed **August 23, 2001**, a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,



Linda S. Chan
Reg. No. 42,400

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.:FUJO 19.208
TELEPHONE: (212) 940-8800

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC973 U.S. PTO
09/998550
11/29/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 8月23日

出 願 番 号

Application Number:

特願2001-253308

出 願 人

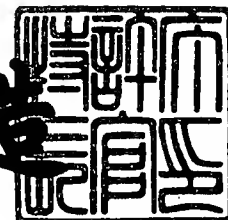
Applicant(s):

富士通株式会社

2001年10月26日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3093370

【書類名】 特許願

【整理番号】 0100036

【提出日】 平成13年 8月23日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/56

【発明の名称】 仮想私設網サービスを提供するシステム

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 鈴木 浩之

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100074099

【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F

【弁理士】

【氏名又は名称】 大菅 義之

【電話番号】 03-3238-0031

【選任した代理人】

【識別番号】 100067987

【住所又は居所】 神奈川県横浜市鶴見区北寺尾7-25-28-503

【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-573-3683

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 仮想私設網サービスを提供するシステム

【特許請求の範囲】

【請求項 1】 複数のルータ装置を含む I P 網を利用して仮想私設網サービスを提供するシステムであって、

上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とする仮想私設網サービスを提供するシステム。

【請求項 2】 請求項 1 に記載のシステムであって、

同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有する。

【請求項 3】 請求項 1 に記載のシステムであって、

第 1 のルータ装置内に設けられた第 1 の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第 1 の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルータユニットから上記第 1 の仮想ルータユニットへ応答情報が返送され、

上記第 1 の仮想ルータユニットは、上記応答情報に基づいて、対応する仮想私設網のネットワーク構成を検出する。

【請求項 4】 請求項 1 に記載のシステムであって、

第 1 のルータ装置内に設けられた第 1 の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第 1 の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルータ

タユニットである第2の仮想ルータユニットから上記第1の仮想ルータユニットへ応答情報が返送され、

上記第1の仮想ルータユニットと上記第2の仮想ルータユニットとの間に上記ルーティング情報を転送するための制御チャネルが設定される。

【請求項5】 IP網を利用して仮想私設網サービスを提供するシステムにおいて使用されるルータ装置であって、

上記仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、
その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とするルータ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、IP網を利用して構築される仮想私設網およびその仮想私設網のために使用されるルータ装置に係わる。

【0002】

【従来の技術】

従来より、多くのユーザが私設網（あるいは、自営網）を構築している。私設網は、あるグループ内の端末装置間のみでのデータ転送を許可するネットワークであり、従来は、一般に、専用線を利用して構築されていた。ところが、近年では、通信コストの削減などの要求により、インターネット等の不特定多数のユーザに開放されているIP網を利用して仮想的な私設網を構築しようとする動きが広がっている。なお、インターネットは、世界中のユーザに広く開放されたIP網であり、多数のルータ装置により構築されている。

【0003】

インターネット上では、データは、基本的に、IPパケットに格納されて転送

される。ここで、各 I P パケットにはそれぞれ宛先アドレスが付与されている。そして、各ルータ装置は、I P パケットを受信すると、付与されている宛先アドレスに従ってその I P パケットの経路を決定する。この場合、経路の決定に際して、ルーティングテーブルが参照される。

【 0 0 0 4 】

ルーティングテーブルは、I P パケットの転送経路を決定するための情報を含んでおり、ルーティングアルゴリズムにより設定および管理される。一例としては、宛先ネットワークとネクストホップとの対応関係を表す情報が登録されている。この場合、ルータ装置は、受信した I P パケットの宛先アドレスを検索キーとしてルーティングテーブルを検索することによりネクストホップを決定し、上記 I P パケットをそのネクストホップへ送出する。そして、経路上の各ルータ装置により上記処理が実行されることにより、I P パケットが宛先アドレスへ転送される。

【 0 0 0 5 】

インターネット上の仮想私設網は、通常、I P トンネリング (IP Tunneling) により実現される。代表的な I P トンネリングとしては、例えば、マイクロソフト社の P P T P (Point-to-Point Tunneling Protocol) や、シスコシステムズ社の L 2 F (Layer 2 Forwarding) などが知られているが、現在では、これら 2 つのプロトコルが融合された L 2 T P (Layer 2 Tunneling Protocol) が普及しつつある。ここで、L 2 T P は、P P P (Point-to-Point Protocol) データをトンネルしながら、データリンク層でそのパケットを暗号化するプロトコルである。なお、L 2 T P は、I E T F (Internet Engineering Task Force) により標準化されており、R F C 2 6 6 1 として制定されている。

【 0 0 0 6 】

【発明が解決しようとする課題】

上述のように、インターネットを利用して仮想私設網を構築する方法は、I E T F などにおいて検討されている。しかし、すべての仕様が議論されているわけではない。例えば、セキュリティを確保する方法については十分な議論がなされているとは言えない。

【0007】

例えば、各ルータ装置は、現状、1つのルーティングテーブルを用いてルーティング処理を行っている。そして、そのルーティングテーブルには、一般ユーザのためのルーティング情報、および仮想私設網サービスユーザのためのルーティング情報が格納されている。すなわち、ルーティングテーブルは、不特定多数のユーザのために共通に利用されるようになっている。

【0008】

このため、ルーティングテーブルに格納されているルーティング情報は、不正アクセスにより盗まれたり、書き換えられたりする危険性がある。すなわち、ルーティング情報が盗まれ、それを解析されると、仮想私設網サービスユーザのネットワーク構成が知られてしまう。また、ルーティング情報を書き換えることにより、特定の仮想私設網内で送受信される情報が盗聴される可能性もある。

【0009】

また、仮想私設網を実現する方法の1つとして、MPLS-VPN (Multi-Protocol Label Switching-Virtual Private Network) が知られている。しかし、この方法では、複数の拠点にそれぞれ設けられているネットワーク（例えば、キャンパスネットワーク）をBGP (Border Gateway Protocol) などを利用して互いに接続しようとする、各ネットワークがそれぞれ独立した自律網 (AS: Autonomous System) となってしまう、全体で1つの自律網を構築することはできない。したがって、複数のネットワークが専用線で接続されている仮想私設網を、インターネットを利用した仮想私設網に移行することは困難である。

【0010】

本発明の目的は、IP網を利用した仮想私設網のセキュリティを向上させることである。

【0011】

【課題を解決するための手段】

本発明の仮想私設網サービスを提供するシステムは、複数のルータ装置を含むIP網を利用する方式であって、上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニット

を有し、その仮想ルータユニットが、対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段とを有する。

【 0 0 1 2 】

上記システムにおいては、仮想私設網ごとにルーティングテーブルが分離されている。そして、そのルーティングテーブルを利用して仮想私設網サービスが提供される。したがって、各仮想私設網のセキュリティが高い。

【 0 0 1 3 】

上記システムにおいて、同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有するようにしてもよい。この構成によれば、ルーティングテーブルを作成するための情報が、仮想私設網ごとに独立に送受信されるので、セキュリティがさらに向上する。

【 0 0 1 4 】

【発明の実施の形態】

図 1 は、実施形態の仮想私設網（VPN：Virtual Private Network）に係わるシステムの構成図である。ここでは、ユーザ A、ユーザ B、ユーザ C に対してそれぞれ仮想私設網サービスが提供されているものとする。

【 0 0 1 5 】

実施形態の仮想私設網は、IP 公衆網であるインターネットを利用して構築される。ここで、IP 公衆網には、多数の通信ノードが設けられており、各ユーザは、それぞれ対応するエッジノード（Edge Node）1 A～1 D に收容される。また、各通信ノード（エッジノード 1 A～1 D を含む）は、例えば、ルータ装置などの通信機器である。なお、IP 公衆網を利用して構築される仮想私設網は、しばしば「IP-VPN」と呼ばれている。

【 0 0 1 6 】

各ユーザ（ユーザ A～ユーザ C）は、それぞれ、複数のサイトに端末装置を有している。たとえば、ユーザ A は、エッジノード 1 A～1 D により管理される各

サイトにそれぞれ端末装置を有している。なお、各サイトには、端末装置が1台だけ設けられていてもよいし、複数の端末装置が接続されたLAN (Local Area Network) が設けられていてもよい。

【 0 0 1 7 】

仮想私設網は、擬似的に閉じたネットワークである。したがって、各仮想私設網内で送受信されるIPパケットは、他の仮想私設網に属する端末装置あるいは一般ユーザの端末装置に転送されることはない。また、仮想私設網内では、IPパケットは、L2TPなどのIPトンネルを利用して転送されてもよいし、MPLS (Multi-Protocol Label Switching) のラベルパスを利用して転送されてもよい。

【 0 0 1 8 】

図2は、実施形態の仮想私設網を構築する方法の概念を説明する図である。ここでは、2台のエッジノードのみを示す。なお、エッジノードは、ルータ装置であるものとする。

【 0 0 1 9 】

ルータ装置10、20は、それぞれ複数のユーザを収容することができる。ここでは、ルータ装置10は、ユーザA、ユーザB、およびユーザCを収容しており、ルータ装置20は、ユーザAおよびユーザBを収容している。また、ルータ装置10、20は、それぞれ各ユーザに対応するVR (Virtual Router) ポートを備えている。この実施例では、ルータ装置10には、ユーザAに対応するVRポート11a、ユーザBに対応するVRポート11b、およびユーザCに対応するVRポート11cが設けられている。同様に、ルータ装置20には、ユーザAに対応するVRポート21a、およびユーザBに対応するVRポート21bが設けられている。なお、各ユーザと対応するVRポートとの間は、基本的に1:1に接続されている。

【 0 0 2 0 】

各VRポートは、それぞれルーティングテーブルを備えている。ここで、このルーティングテーブルは、仮想私設網ごとに作成される。すなわち、VRポート11aが備えるルーティングテーブル12aおよびVRポート21aが備えるル

ーティングテーブル 2 2 a には、ユーザ A の仮想私設網のためのルーティング情報のみが格納されている。同様に、ルーティングテーブル 1 2 b、2 2 b にはユーザ B の仮想私設網のためのルーティング情報のみが格納されており、ルーティングテーブル 1 2 c にはユーザ C の仮想私設網のためのルーティング情報のみが格納されている。

【 0 0 2 1 】

また、各 VR ポートは、同一の仮想私設網に属する VR ポートのみとの間でルーティング情報などの制御情報を交換する。このとき、これらの制御情報は、L 2 T P などにより形成される IP トンネルを介して送受信される。例えば、VR ポート 1 1 a は、VR ポート 2 1 a との間に L 2 T P トンネルを形成できるが、他の VR ポートとの間にはそれを形成することはできない。従って、この場合、VR ポート 1 1 a のルーティングテーブル 1 2 a に格納されているルーティング情報は、L 2 T P トンネルを介して VR ポート 2 1 a のみに送られる。また、このとき、VR ポート 1 1 a は、VR ポート 2 1 a のルーティングテーブル 2 2 a に格納されているルーティング情報を L 2 T P トンネルを介して受け取ることができる。そして、各 VR ポートでは、交換されたルーティング情報により、ルーティング情報が作成／更新される。

【 0 0 2 2 】

なお、エッジノード間でルーティング情報を送受信する方法は、公知の技術を利用することができ、例えば、O S P F (Open Shortest Path First) により実現されてもよい。この場合、一方のエッジノードから他方のエッジノードへ情報が送られる際に、その経路上に設けられているルータ装置のルーティングテーブルが更新される。そして、本実施形態では、各 VR ポートがエッジノードとして動作する。すなわち、VR ポート間でルーティング情報が交換され、それらの VR ポートに設けられているルーティングテーブル、および経路上の各ルータ装置に設けられているルーティングテーブルが作成／更新される。

【 0 0 2 3 】

一例を示す。ここでは、VR ポート 1 1 a と VR ポート 2 1 a との間でルーティング情報が交換される場合を想定する。例えば、VR ポート 2 1 a から VR ポ

ート 1 1 a へ転送されるルーティング情報は、「サイト A 3 に設けられているユーザ A の端末装置宛てのパケットは、ルータ装置 2 0 の V R ポート 2 1 a に転送される。」を含んでいる。この場合、図 3 に示すように、V R ポート 1 1 a のルーティングテーブル、および V R ポート 2 1 a と V R ポート 1 1 a との間の経路上に設けられている各ルータ装置のルーティングテーブルが更新される。具体的には、ルータ Y のルーティングテーブルには、サイト A 3 のユーザ A 宛てのパケットを V R ポート 2 1 a へ転送するための情報が登録される。また、ルータ X のルーティングテーブルには、サイト A 3 のユーザ A 宛てのパケットをルータ Y へ転送するための情報が登録される。さらに、V R ポート 1 1 a のルーティングテーブル 1 2 a には、サイト A 3 のユーザ A 宛てのパケットをルータ X へ転送するための情報が登録される。同様に、V R ポート 1 1 a から V R ポート 2 1 a へ転送されるルーティング情報は、「サイト A 1 に設けられているユーザ A の端末装置宛てのパケットは、ルータ装置 1 0 の V R ポート 1 1 a に転送される。」を含んでいる。

【 0 0 2 4 】

このように、実施形態のルータ装置は、仮想私設網ごとに V R ポートを備えている。ここで、各 V R ポートは、対応する仮想私設網のためのルーティング情報を管理しており、また、同一の仮想私設網に属する V R ポートのみとの間でそのルーティング情報を交換する。これにより、仮想私設網ごとにルーティング情報が分離され、各仮想私設網のセキュリティが向上する。

【 0 0 2 5 】

仮想私設網内で送受信されるパケットのルーティング処理は、対応する V R ポートにより行われる。例えば、サイト A 1 に設けられているユーザ A の端末装置からサイト A 3 に設けられているユーザ A の端末装置宛てのパケットが送出されると、そのパケットは、まず、ルータ装置 1 0 の V R ポート 1 1 a により受信される。V R ポート 1 1 a は、受信したパケットの宛先きアドレスを検索キーとしてルーティングテーブル 1 2 a からルーティング情報を取り出し、そのルーティング情報に従って上記パケットを送出する。この場合、上記パケットは、図 3 に示したルーティング情報に従って、ルータ X、ルータ Y を介して V R ポート 2 1

a へ転送される。そして、VRポート21aが、そのパケットをサイトA3のユーザAへ転送する。このように、端末装置間で送受信されるパケットは、VRポートにより形成される仮想私設網内を転送される。

【0026】

なお、図3では、一般的なルーティングテーブルを示したが、ラベル付きのルーティングテーブルであっても、その作成／更新手順は基本的に同じである。

図4は、仮想私設網を提供するルーティングエリアの構造を模式的に示す図である。ルーティングエリアは、階層的な構造を有しており、制御プレーンおよびユーザプレーンから構成される。制御プレーンは、VRポート間で制御情報を送受信するためのエリアである。なお、制御情報は、上述したように、仮想私設網ごとに形成されるトンネルを介して送受信されるので、仮想私設網ごとに互いに分離されている。一方、ユーザプレーンは、主信号（端末装置間で送受信されるデータ）を送受信するためのエリアである。ここで、ルータ装置は、上述したように、仮想私設網ごとに設けられるVRポートを備えている。また、各仮想私設網内の主信号は、対応するVRポートによりルーティングされる。したがって、ユーザプレーンは、仮想私設網ごとのプレーンに分離されている。

【0027】

図5は、実施形態のルータ装置の構成図である。ここで、このルータ装置は、複数のユーザ回線および他のルータ装置に接続される局間回線を収容している。そして、各ユーザ回線は、それぞれ対応するVRポートに接続されている。

【0028】

ルータ装置は、上述したように、1または複数のVRポート30を備える。そして、VRポート30は、ゲートウェイプロトコルデーモン31、ルーティングテーブル32、制御チャネル終端部33、VPN構成モジュール34、ラベル付与部36などを備える。

【0029】

ゲートウェイプロトコルデーモン31は、ルータ装置の基本動作を提供する。具体的には、ルーティングテーブルを作成／更新する処理、パケットのルートを決定する処理などを実行する。なお、ゲートウェイプロトコルデーモン31は、

例えば、MPLS (Multi-Protocol Label Switching) ネットワークを介してIPパケットを転送する機能を備える。また、ゲートウェイプロトコルデーモン31は、プライベートアドレスとグローバルアドレスとを相互に変換する機能を備えていてもよい。

【0030】

ルーティングテーブル32には、対応する仮想私設網のためのルーティング情報が格納される。ここで、ルーティングテーブル32は、所定のルーティングアルゴリズムにより設定／管理される。一例としては、図6(a)に示すように、宛先ネットワークとネクストホップの組合せが登録されている。この場合、ルータ装置(VRポート)は、受信したIPパケットの宛先アドレスを検索キーとしてルーティングテーブルを検索することによりネクストホップを決定し、上記IPパケットをそのネクストホップへ送出する。なお、ルーティングテーブルの構造は、特に限定されるものではない。

【0031】

制御チャネル終端部33は、VRポート間で制御情報(ルーティング情報等)を伝送するための制御チャネルを終端する。ここで、制御チャネルは、L2TPトンネルにより実現される。したがって、制御チャネル終端部33は、L2TPクライアントおよびL2TPサーバを備える。L2TPクライアントは、L2TPトンネルの設定を要求するプログラムユニットである。一方、L2TPサーバは、L2TPクライアントからの要求に従ってL2TPトンネルを形成するプログラムユニットである。

【0032】

VPN構成モジュール34は、上記制御チャネルが設定されるときに、その制御チャネルに接続されるVRポートを認証する。このため、VPN構成モジュール34は、RADIUSクライアントおよびRADIUSサーバを備える。RADIUSクライアントは、VRポートの認証を要求するプログラムユニットである。一方、RADIUSサーバは、RADIUSクライアントからの要求に従ってVRポートを認証するプログラムユニットである。

【0033】

また、VPN構成モジュール34は、上記制御チャネルを監視／制御する機能を備える。具体的には、例えば、定期的に制御チャネルを介して監視メッセージを送出し、対応するVRポートから応答メッセージを受信できるか否かをモニタする。そして、応答メッセージを受信できなかったときに、その制御チャネルを削除する処理などを行う。

【0034】

さらに、VPN構成モジュール34は、対応する仮想私設網の構成を定義するVPN構成マップ36を作成する。VPN構成マップ36は、少なくとも、対応する仮想私設網に係わるルータ装置を識別するルータIDのリストを含む。ここで、「仮想私設網に係わるルータ装置」とは、その仮想私設網に属する端末装置を収容するルータ装置のことをいう。また、VPN構成マップ36は、図6(b)に示すように、その端末装置を収容するVRポートのIPアドレスが登録される構成であってもよい。

【0035】

ラベル付与部36は、MPLSのラベルスイッチのためのラベルをIPパケットに付与する。なお、ラベルスイッチは、公知の技術であり、例えば、タグスイッチ(RFC2105)や、セルスイッチルータ(RFC2098)などが知られている。

【0036】

ラベルマトリクス37は、VRポートから出力されたIPパケットをラベルに従って対応する局間回線に導く。また、局間回線から入力されたIPパケットをラベルに対応するVRポートに導く。

【0037】

このように、実施形態のシステムでは、主信号(端末装置間で送受信されるデータ)はMPLSネットワークを介して伝送される。しかし、MPLSのラベルパスは、仮想私設網ごとに設けられたVRポートにより設定される。このため、各ラベルパスは、仮想私設網ごとにVRポート内で閉じている。したがって、仮想私設網内のユーザデータが盗聴されることはない。

【0038】

図 7 は、V R ポートが増設される際のシーケンスを説明する図である。ここでは、ユーザ A の仮想私設網（以下、仮想私設網 A）のために、V R ポート（A1）および V R ポート（A2）が既に設けられているものとする。そして、この仮想私設網を拡張するために、V R ポート（A3）が追加（増設）されるものとする。

【 0 0 3 9 】

なお、各 V R ポートには、それぞれ対応する仮想私設網を識別する V P N 識別子が付与されている。例えば、V R ポート（A1）～（A3）には、それぞれ仮想私設網 A を識別する V P N 識別子が付与されている。また、各 V R ポートには、それぞれ I P アドレスが割り当てられている。

【 0 0 4 0 】

この場合、まず、V R ポート（A3）は、すべてのルータ装置に対して増設メッセージをブロードキャストする。この増設メッセージは、仮想私設網 A を識別する V P N 識別子、V R ポート（A3）を収容するルータ装置を識別するルータ識別子、および V R ポート（A3）に割り当てられている I P アドレスを含んでいる。そして、この増設メッセージは、各ルータ装置の各 V R ポートによって受信される。

【 0 0 4 1 】

V R ポート（A1）および V R ポート（A2）は、増設メッセージを受信すると、対応する応答（A C K）メッセージを V R ポート（A3）へ返送する。この応答メッセージには、増設メッセージと同様に、V P N 識別子、ルータ識別子および当該 V R ポートの I P アドレスを含んでいる。なお、仮想私設網 A を識別する V P N 識別子が付与されていない V R ポートは、上記増設メッセージを受信しても、応答メッセージを返送しない。図 7 に示す例では、V R ポート（B）は、応答メッセージを返送しない。

【 0 0 4 2 】

V R ポート（A3）は、受信した応答メッセージに基づいて、仮想私設網 A の構成を表す V P N 構成マップを作成する。この実施例では、仮想私設網 A に V R ポート（A1）および V R ポート（A2）が属していることが認識され、その認識結果に対応する V P N 構成マップが作成される。

【 0 0 4 3 】

続いて、VRポート (A3) と VRポート (A1) との間、及び VRポート (A3) と VRポート (A2) との間にそれぞれ L 2 T P トンネルが設定される。そして、それらの L 2 T P トンネルを介して、それぞれルーティング情報が交換される。これにより、VRポート (A3) において、ルーティングテーブルが作成される。一方、VRポート (A1) および VRポート (A2) では、それぞれルーティングテーブルが更新される。

【 0 0 4 4 】

このように、新たな VRポートが追加されると、その新たな VRポートと既存の VRポートとの間でルーティング情報が交換され、ルーティングテーブルが作成／更新される。ここで、ルーティング情報の交換は、同じ仮想私設網に属する VRポートの間で行われる。しかも、そのルーティング情報は、それらの VRポート間に設定される L 2 T P トンネルを介して転送される。したがって、各仮想私設網のセキュリティは高い。

【 0 0 4 5 】

図 8 は、新たに追加された VRポートにおいてルーティングテーブルを作成する処理のフローチャートである。以下では、図 7 に示したシーケンスを参照しながら説明する。すなわち、図 7 に示したシーケンスにおける VRポート (A3) の動作を説明する。

【 0 0 4 6 】

ステップ S 1 では、増設メッセージをすべてのルータ装置にブロードキャストする。この増設メッセージは、上述したように、仮想私設網 A を識別する VPN 識別子、VRポート (A3) を収容するルータ装置を識別するルータ識別子、および VRポート (A3) に割り当てられている IP アドレスを含んでいる。

【 0 0 4 7 】

ステップ S 2 では、ステップ S 1 で送出した増設メッセージに対応する応答メッセージを受信する。なお、この応答メッセージは、仮想私設網 A に属する VRポートのみから返送されてくる。

【 0 0 4 8 】

ステップ S 3 では、受信した応答メッセージから必要な情報を取得する。具体的には、応答メッセージを送出した V R ポートの I P アドレス、およびその V R ポートを収容するユーザ装置のルータ識別子などを取得する。

【 0 0 4 9 】

ステップ S 4 では、ステップ S 3 で取得した情報に基づいて V P N 構成マップを作成する。この V P N 構成マップは、仮想私設網 A の構成を表し、一例としては図 6 (b) に示した通りである。

【 0 0 5 0 】

ステップ S 5 ～ S 9 の処理は、応答メッセージを送出した各 V R ポートについてそれぞれ実行される。図 7 に示す例では、V R ポート (A1) および V R ポート (A2) についてそれぞれ実行される。以下では、V R ポート (A1) について実行する場合を説明する。

【 0 0 5 1 】

ステップ S 5 では、V R ポート (A1) との間に L 2 T P トンネルを設定するために、L 2 T P クライアントおよび R A D I U S クライアントが起動される。このとき、V R ポート (A3) を認証するために必要な情報が V R ポート (A1) に送られる。そして、V R ポート (A1) において V R ポート (A3) の認証が成功すると、V R ポート (A3) と V R ポート (A1) との間に L 2 T P トンネルが設定される。この場合、この L 2 T P トンネルを識別するトンネル識別子が決定され、以降、V R ポート (A3) および V R ポート (A1) によりそのトンネル識別子がそれぞれ管理される。なお、上記認証に失敗した場合には、処理を終了する (ステップ S 6)。

【 0 0 5 2 】

ステップ S 7 では、ステップ S 5 において設定した L 2 T P トンネルを利用して、V R ポート (A1) との間でルーティング情報を交換する。具体的には、V R ポート (A1) のルーティングテーブルに格納されているルーティング情報を取得する。また、V R ポート (A3) が既にルーティングテーブルを備えている場合には、そのテーブルに格納されているルーティング情報を V R ポート (A1) へ送信する。

【 0 0 5 3 】

ステップ S 8 では、ルーティングテーブルを作成し、ステップ S 7 で受信したルーティング情報をそのテーブルに登録する。なお、この時点で既にルーティングテーブルが作成されている場合には、受信したルーティング情報によりそのテーブルが更新される。この後、ステップ S 9 において、未処理の VR ポートが残っていないかがチェックされ、残っていた場合にはステップ S 5 に戻る。

【 0 0 5 4 】

図 9 は、新たな VR ポートが追加されたときの既設の VR ポートの動作を説明するフローチャートである。以下では、図 7 に示した VR ポート (A1)、VR ポート (A2)、または VR ポート (B) の動作を説明する。

【 0 0 5 5 】

ステップ S 1 1 では、VR ポート (A3) から増設メッセージを受信する。この増設メッセージは、上述した通りである。

ステップ S 1 2 では、当該 VR ポートが属する仮想私設網を識別する VPN 識別子と、受信した増設メッセージに設定されている VPN 識別子とを比較する。そして、それらが一致すれば、仮想私設網 A の中で VR ポートが増設されたものとみなし、ステップ S 1 3 へ進む。一方、それらが互いに一致しなかった場合には、処理を終了する。

【 0 0 5 6 】

ステップ S 1 3 では、受信した増設メッセージから必要な情報を取得する。具体的には、増設メッセージを送出した VR ポートの IP アドレス、およびその VR ポートを収容するユーザ装置のルータ識別子などを取得する。そして、ステップ S 1 4 において、応答メッセージを作成し、それを VR ポート (A3) へ返送する。

【 0 0 5 7 】

ステップ S 1 5 では、要求された L 2 T P トンネルを設定するために、L 2 T P サーバおよび R A D I U S サーバが起動される。なお、この処理は、L 2 T P クライアントからのセットアップ要求および R A D I U S クライアントからの認証要求を受信したときに実行される。この実施例では、VR ポート (A3) を認証

する旨の要求を受信する。

【 0 0 5 8 】

VRポート (A3) の認証に成功した場合は、ステップ S 1 7 ~ S 1 9 の処理が実行され、失敗した場合は、ステップ S 2 1 において、対応するエラー処理が行われる。

【 0 0 5 9 】

ステップ S 1 7 では、ステップ S 1 3 で取得した情報に基づいてVPN構成マップを作成する。このVPN構成マップは、仮想私設網Aの構成を表し、一例としては図6 (b) に示した通りである。

【 0 0 6 0 】

ステップ S 1 8 では、ステップ S 1 5 において設定したL2TPトンネルを利用して、VRポート (A3) との間でルーティング情報を交換する。具体的には、当該VRポートのルーティングテーブルに格納されているルーティング情報をVRポート (A3) へ送信する。また、VRポート (A3) が既にルーティングテーブルを備えている場合には、そのテーブルに格納されているルーティング情報を受け取る。そして、ステップ S 1 9 において、ステップ S 1 8 で受信したルーティング情報によりルーティングテーブルを更新する。

【 0 0 6 1 】

このように、仮想私設網を拡張するためにVRポートが追加されると、そのVRポートと当該仮想私設網に属する他のVRポートとの間にIPトンネルが設定される。そして、そのIPトンネルを介してルーティング情報が送受信される。したがって、各ルータ装置において、仮想私設網ごとにルーティングテーブルが作成される。これにより、仮想私設網のセキュリティが向上する。

【 0 0 6 2 】

なお、上述の実施例では、VRポート間でルーティング情報を転送するためのIPトンネルとしてL2TPトンネルが使用されているが、これに限定されるものではない。また、上述の実施例では、認証プロトコルとしてRADIUSが使用されているが、これに限定されるものではない。さらに、上述の実施例では、既設のVRポートが新たに追加されたVRポートを認証する方式であるが、既設

のVRポートおよび新たに追加されたVRポートが相互に認証する方式であってもよい。

【0063】

次に、VRポートが削除された場合の処理を説明する。仮想私設網を縮小する場合には、対応するVRポートが削除される。例えば、複数のLANがIP網を利用して接続されている仮想私設網において、あるLANを廃止または切り離す場合には、そのLANに対応するVRポートが削除される。この場合、残されたVRポートは、削除されたVRポートとの間に設定されているL2TPトンネルを消滅させたり、ルーティングテーブルを更新したりする必要がある。

【0064】

図10は、あるVRポートが削除されたときに残されたVRポートの処理を示すフローチャートである。ここでは、図7～図9の手順により、同一仮想私設網内のVRポート間にルーティング情報を転送するためのL2TPトンネルが設定されているものとする。また、このフローチャートの処理は、定期的に行われるものとする。

【0065】

ステップS31では、L2TPトンネルの状態を監視する。L2TPトンネルの状態は、例えば、そのトンネルに接続される一方のVRポートから他方のVRポートに監視メッセージを送出し、それに対応する応答メッセージが返送されてくるか否かにより判断される。そして、監視メッセージを送出したVRポートが対応する応答メッセージを受信できたときは、L2TPトンネルが正常であると判断される。なお、複数のL2TPトンネルが設定されている場合は、各トンネルについて同様の処理が行われる。

【0066】

L2TPトンネルが正常でなかった場合は、ステップS32において、対向するVRポートが削除された可能性があるものと判断し、ステップS33以降の処理が実行される。

【0067】

ステップS33では、タイマが起動される。ステップS34及びS35では、

上記タイマの起動開始から所定時間（例えば、24時間）内に、対向するVRポートが復旧したか否かを調べる。対向するVRポートが復旧したか否かは、上述の監視メッセージを使用して判断することができる。そして、所定時間内に対向するVRポートが復旧した場合には、タイマが解除され、処理が終了する。

【0068】

一方、所定時間内に対向するVRポートが復旧しなかった場合には、ステップS36において、上記VRポートとの間に設定されている制御チャネル（L2TPトンネル）を削除する。制御チャネルの削除に際しては、例えば、L2TPトンネルを規定する各種パラメータが解放される。

【0069】

ステップS37では、VPN構成マップを更新する。具体的には、VPN構成マップから、削除されたVRポートに係わる情報を削除する。続いて、ステップS38では、同一仮想私設網に属する残されたVRポート間で、ルーティング情報を交換する。そして、ステップS39において、交換されたルーティング情報によりルーティングテーブルが更新される。

【0070】

このように、ある仮想私設網に属するVRポートが削除されると、その仮想私設網に属する他のVRポートにおいて、削除されたVRポートに接続されていた制御チャネルが削除される。そして、残されたVRポートにおいて、必要に応じてルーティングテーブルが更新される。

【0071】

図11および図12は、仮想私設網の構築例を示す図である。図11に示す例では、仮想私設網サービスを受けるユーザは、複数の営業拠点を持つ私企業である。そして、ユーザごとに、各営業拠点に設けられているキャンパスネットワークが仮想私設網により互いに接続されている。

【0072】

図12に示す例では、仮想私設網サービスを受けるユーザは、複数のアクセスポイントを持つISP（Internet Service Provider）である。そして、ISPごとに、仮想私設網が構築されている。

【0073】

なお、本発明において、「ルーティング情報」は、IP層のルーティングプロトコルで転送される情報に限定されず、IPパケットのルートを決断するための情報をすべて含むものとする。例えば、「ルーティング情報」は、MPLSのラベルパスを設定するための情報を含む。なお、ラベルパスの設定は、例えば、LDP (Label Distribution Protocol) により実現することができる。

【0074】

図13は、VRポート間でラベルパスを設定する手順の例である。ここでは、図3に示したケースと同様に、VRポート11aとVRポート21aとの間でラベルパスのためのルーティング情報が交換される場合を想定する。例えば、VRポート21aからVRポート11aへ転送されるルーティング情報は、「サイトA3に設けられているユーザAの端末装置宛てのパケットは、ラベルFである」を含んでいる。この場合、この情報を受け取ったルータXは、「サイトA3に設けられているユーザAの端末装置宛てのパケットは、ラベルEである」を含むルーティング情報をVRポート11aへ送る。これにより、VRポート11aおよびルータXでは、それぞれ図13に示すようなテーブルが作成される。

【0075】

なお、これらのルーティング情報は、上述の実施例と同様に、VRポート11aとVRポート21aとの間に設定されたIPトンネルを介して転送される。

上記テーブルが作成された後、サイトA1に設けられているユーザAの端末装置からサイトA3に設けられているユーザAの端末装置宛てのパケットが送出されると、そのパケットは、まずルータ装置10のVRポート11aにより受信される。VRポート11aは、そのパケットに「ラベルE」を付与してルータXへ送出する。ルータXは、そのパケットを受け取ると、ラベルを「E」から「F」に書き換えた後、そのパケットをVRポート21aへ送出する。そして、VRポート21aが、そのパケットをサイトA3のユーザAへ転送する。

【0076】

(付記1) 複数のルータ装置を含むIP網を利用して仮想私設網サービスを提供するシステムであって、

上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とする仮想私設網サービスを提供するシステム。

【 0 0 7 7 】

(付記 2) 付記 1 に記載のシステムであって、

同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有する。

【 0 0 7 8 】

(付記 3) 付記 2 に記載のシステムであって、

上記制御チャネルは、IP トンネルである。

(付記 4) 付記 1 に記載のシステムであって、

第 1 のルータ装置内に設けられた第 1 の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第 1 の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルータユニットから上記第 1 の仮想ルータユニットへ応答情報が返送され、

上記第 1 の仮想ルータユニットは、上記応答情報に基づいて、対応する仮想私設網のネットワーク構成を検出する。

【 0 0 7 9 】

(付記 5) 付記 1 に記載のシステムであって、

第 1 のルータ装置内に設けられた第 1 の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第 1 の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルー

タユニットである第2の仮想ルータユニットから上記第1の仮想ルータユニットへ応答情報が返送され、

上記第1の仮想ルータユニットと上記第2の仮想ルータユニットとの間に上記ルーティング情報を転送するための制御チャネルが設定される。

【0080】

(付記6) 付記5に記載のシステムであって、

上記第1の仮想ルータユニットは、当該第1の仮想ルータユニットの認証を要求する認証クライアント手段を有し、

上記第2の仮想ルータユニットは、上記認証クライアントからの要求に応じて上記第1の仮想ルータユニットの認証を実行する認証サーバ手段を有する。

【0081】

(付記7) 付記2に記載のシステムであって、

ある仮想私設網に属する複数の仮想ルータユニットの中の1つが削除されたときに、その削除された仮想ルータユニットに接続されていた制御チャネルが削除され、さらに残された仮想ルータユニットにおいて上記仮想私設網のネットワーク構成を表す構成マップが更新される。

【0082】

(付記8) 付記7に記載のシステムであって、

上記制御チャネルが削除されてから所定時間が経過した後に上記構成マップが更新される。

【0083】

(付記9) IP網を利用して仮想私設網サービスを提供するシステムにおいて使用されるルータ装置であって、

上記仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、
その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とするルータ装置。

【 0 0 8 4 】

【発明の効果】

本発明によれば、仮想私設網ごとにルーティングテーブルが作成されるので、各仮想私設網のセキュリティが向上する。

【図面の簡単な説明】

【図 1】

実施形態の仮想私設網に係わるシステムの構成図である。

【図 2】

実施形態の仮想私設網を構築する方法の概念を説明する図である。

【図 3】

ルーティングテーブルの更新の一例を示す図である。

【図 4】

仮想私設網を提供するルーティングエリアの構造を模式的に示す図である。

【図 5】

実施形態のルータ装置の構成図である。

【図 6】

(a) はルーティングテーブルの例、(b) は V P N 構成マップの例である。

【図 7】

V R ポートが増設される際のシーケンスを説明する図である。

【図 8】

新たに追加された V R ポートにおいてルーティングテーブルを作成する処理のフローチャートである。

【図 9】

新たな V R ポートが追加されたときの既設の V R ポートの動作を説明するフローチャートである。

【図 1 0】

ある V R ポートが削除されたときに残された V R ポートの処理を示すフローチャートである。

【図 1 1】

仮想私設網の構築例（その 1）である。

【図 1 2】

仮想私設網の構築例（その 2）である。

【図 1 3】

VR ポート間でラベルパスを設定する手順の例である。

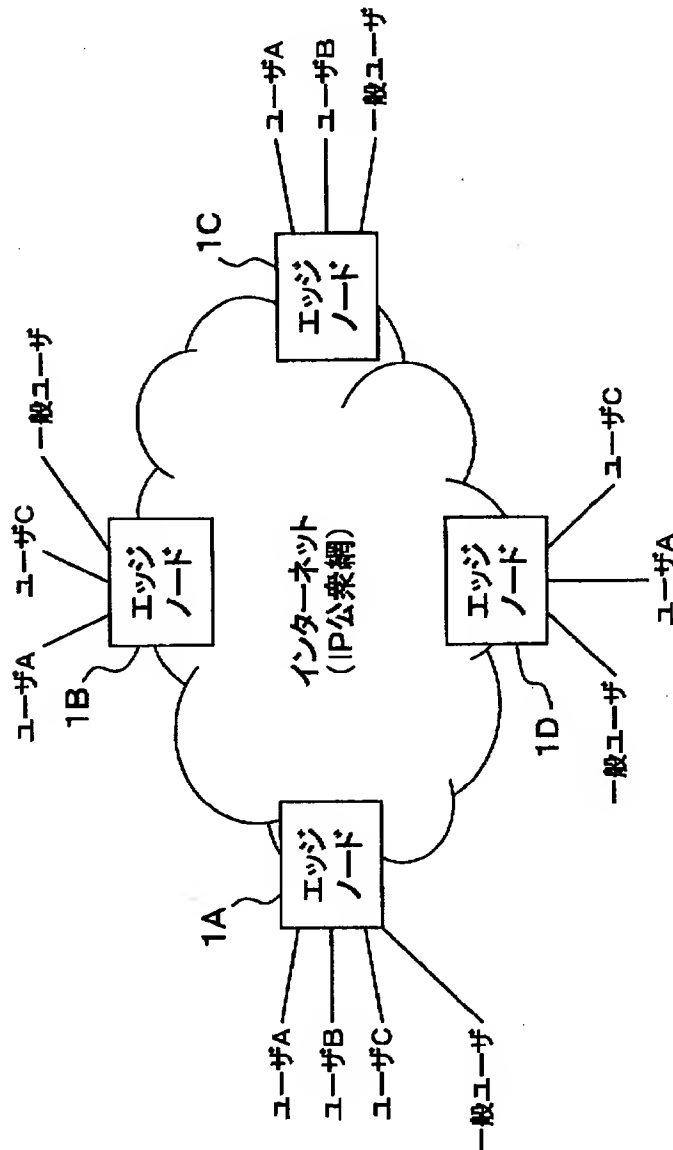
【符号の説明】

| | |
|---------------|-----------------|
| 1 A ～ 1 D | エッジノード |
| 1 0、2 0 | ルータ装置 |
| 1 1 a ～ 1 1 c | VR ポート |
| 1 2 a ～ 1 2 c | ルーティングテーブル |
| 2 1 a ～ 2 1 b | VR ポート |
| 2 2 a ～ 2 2 b | ルーティングテーブル |
| 3 0 | VR ポート |
| 3 1 | ゲートウェイプロトコルデーモン |
| 3 2 | ルーティングテーブル |
| 3 3 | 制御チャネル終端部 |
| 3 4 | VPN 構成モジュール |
| 3 5 | VPN 構成マップ |

【書類名】 図面

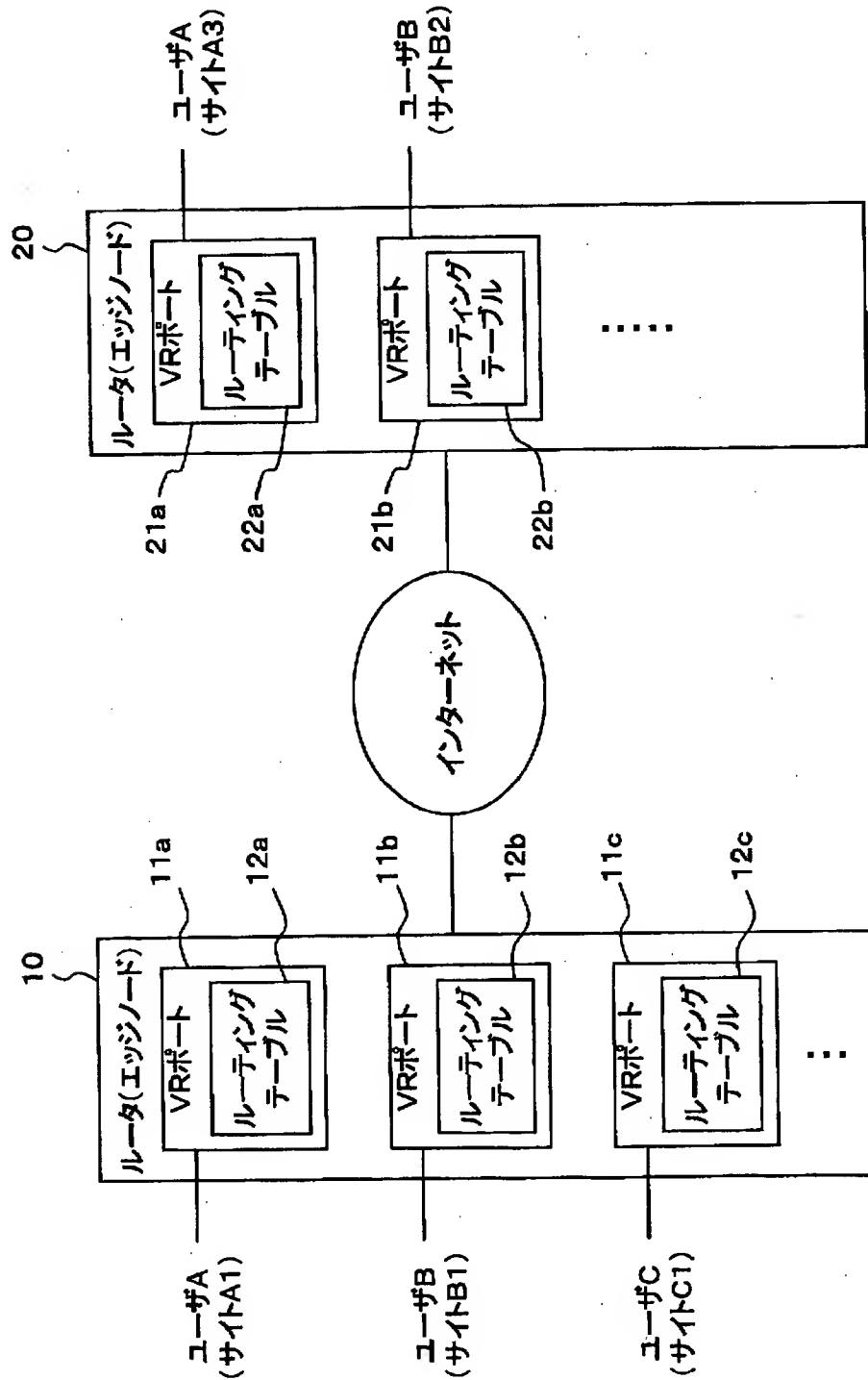
【図1】

実施形態の仮想私設網に係わるシステムの構成図



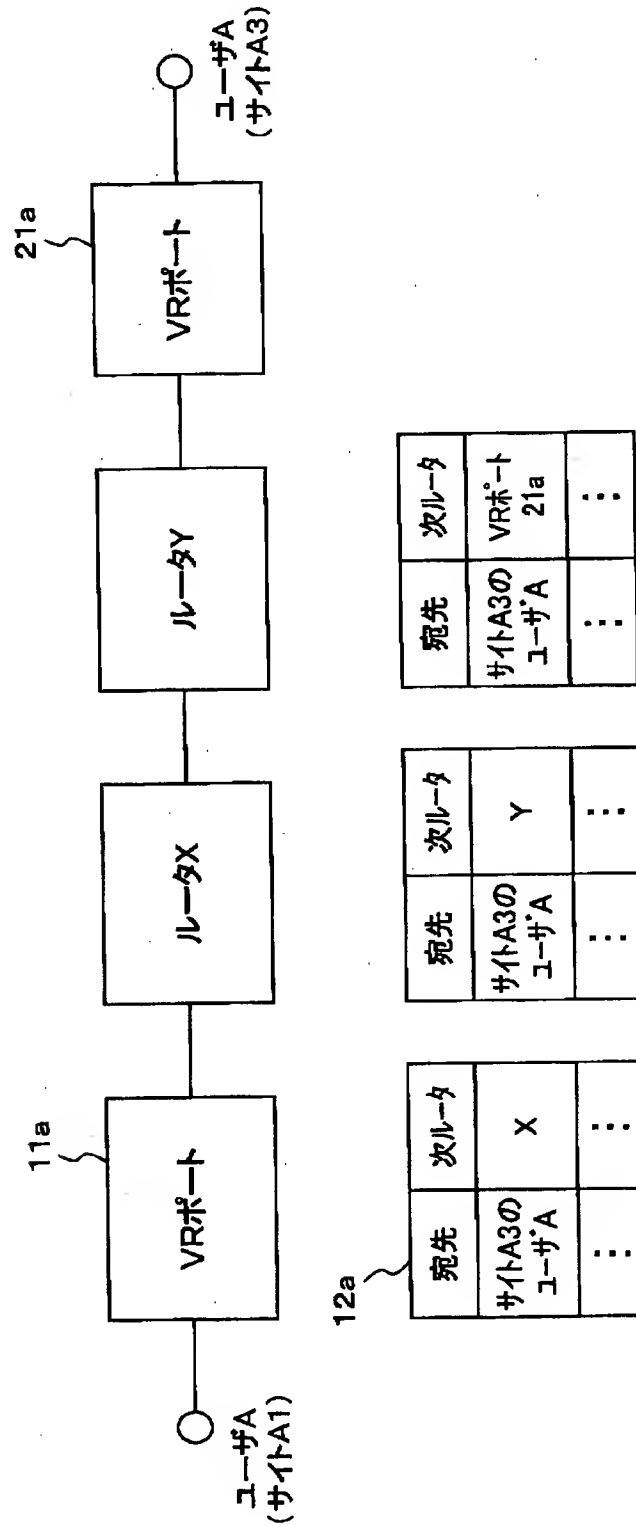
【図 2】

実施形態の仮想私設網を構築する方法の概念を説明する図



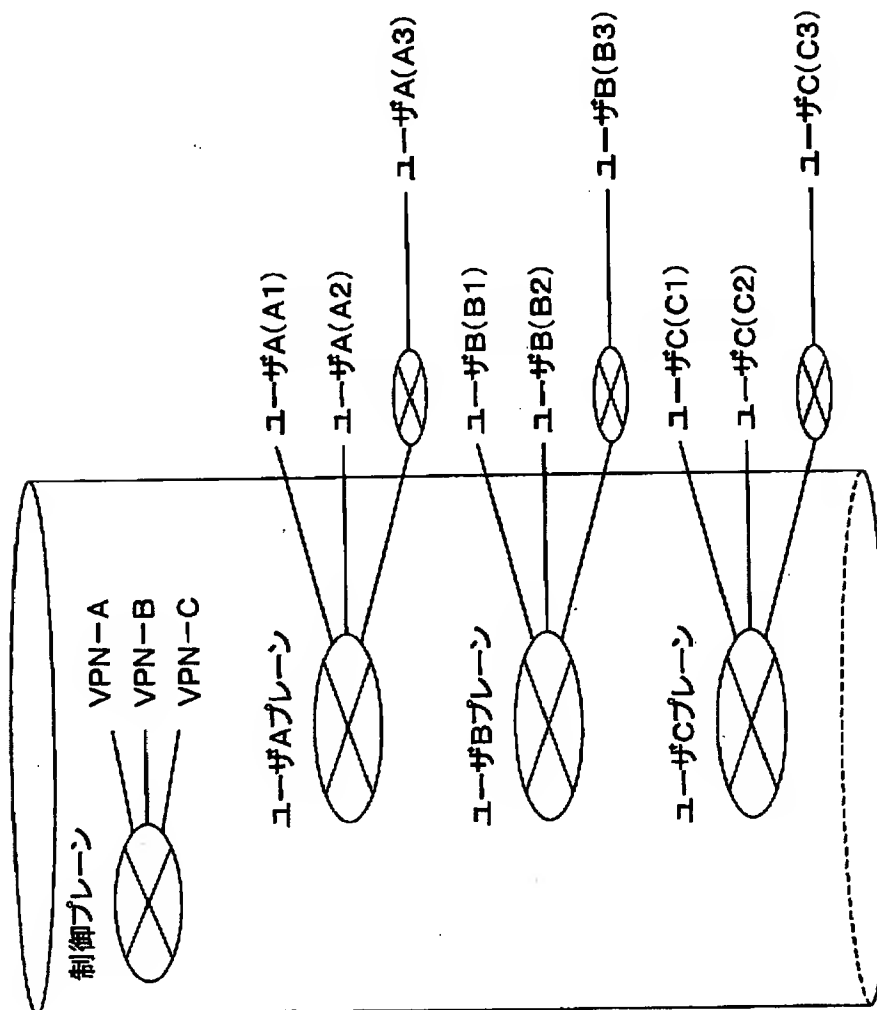
【図 3】

ルーティングテーブルの更新の一例を示す図



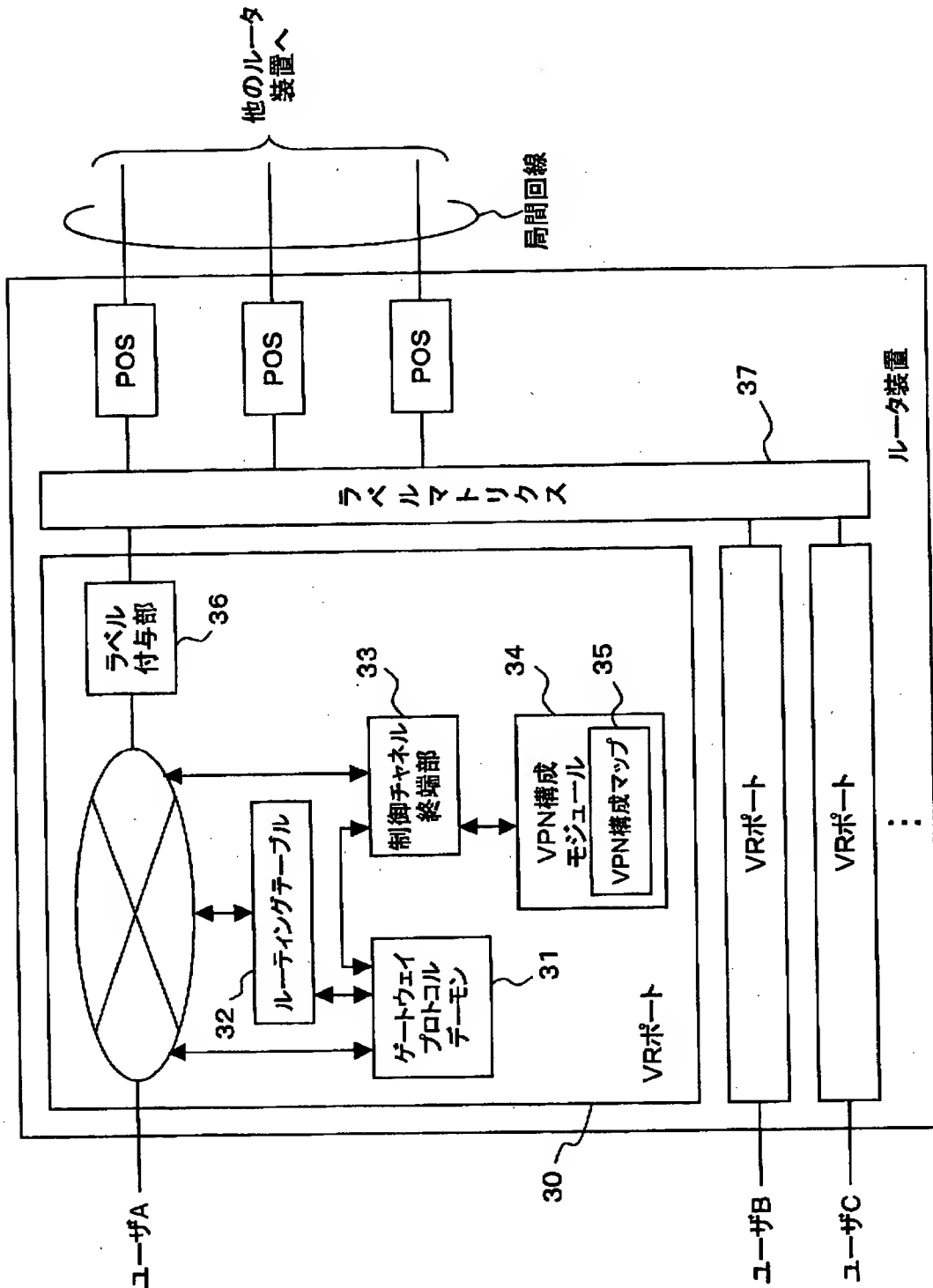
【図 4】

仮想私設網を提供するルーティングエリアの
構造を模式的に示す図



【図 5】

実施形態のルータ装置の構成図



【図 6】

(a) はルーティングテーブルの例、(b) はVPN構成マップの例

(a)

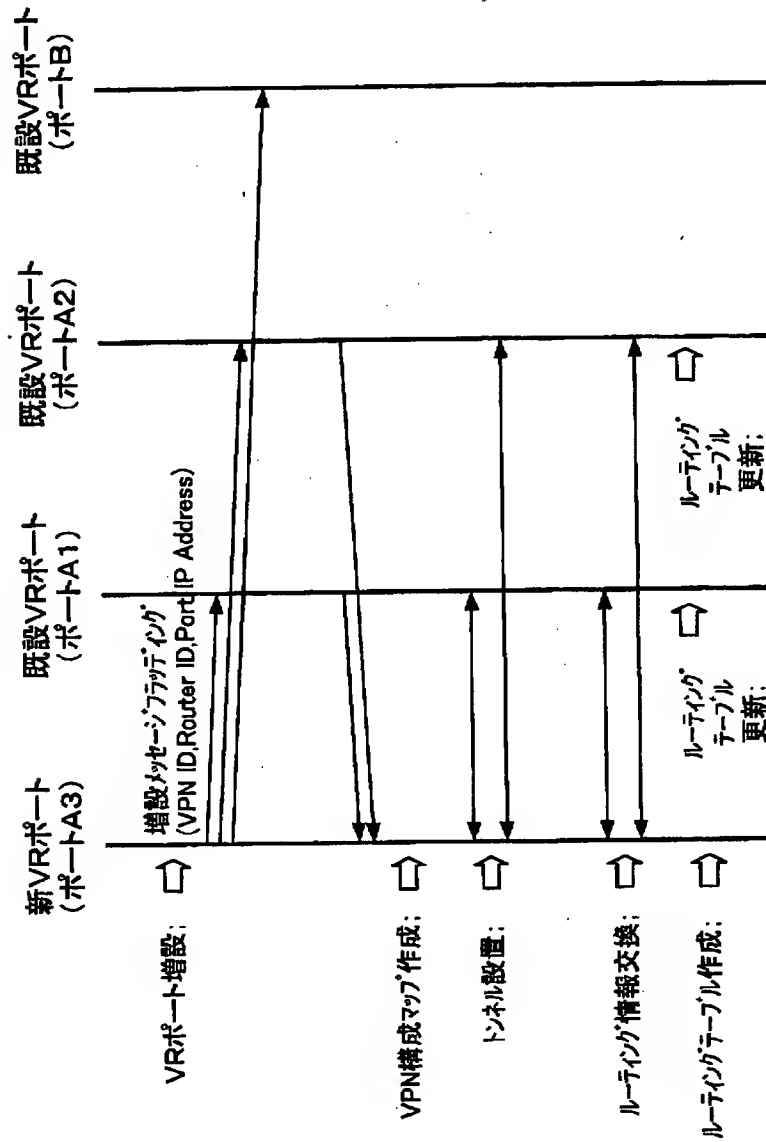
| 宛先ネットワーク | ネクストホップ |
|----------|---------|
| 13 | ノードA |
| 52 | ノードC |
| 14 | ノードA |
| 27 | ノードB |
| 28 | ノードB |
| ⋮ | ⋮ |

(b)

| ルータID | IPアドレス |
|-------|---------|
| 1053 | アドレスabc |
| 0022 | アドレスxyz |
| 0134 | アドレスaax |
| ⋮ | ⋮ |

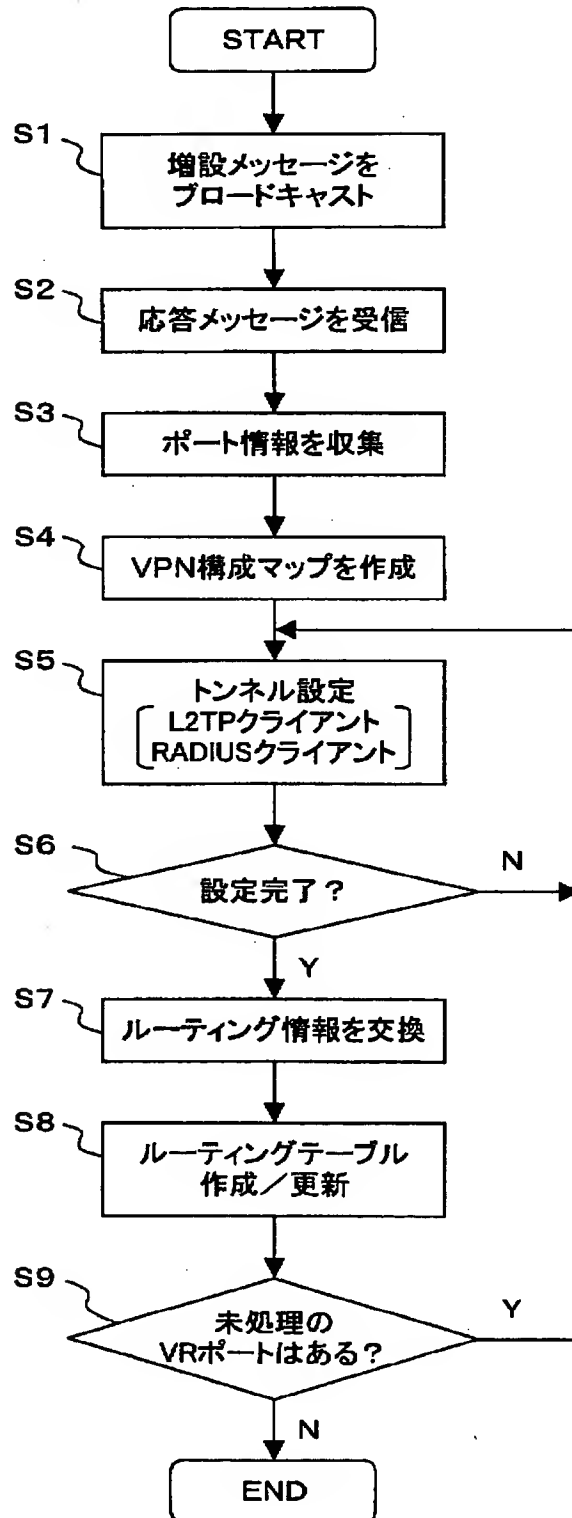
【図 7】

VRポートが増設される際のシーケンスを説明する図



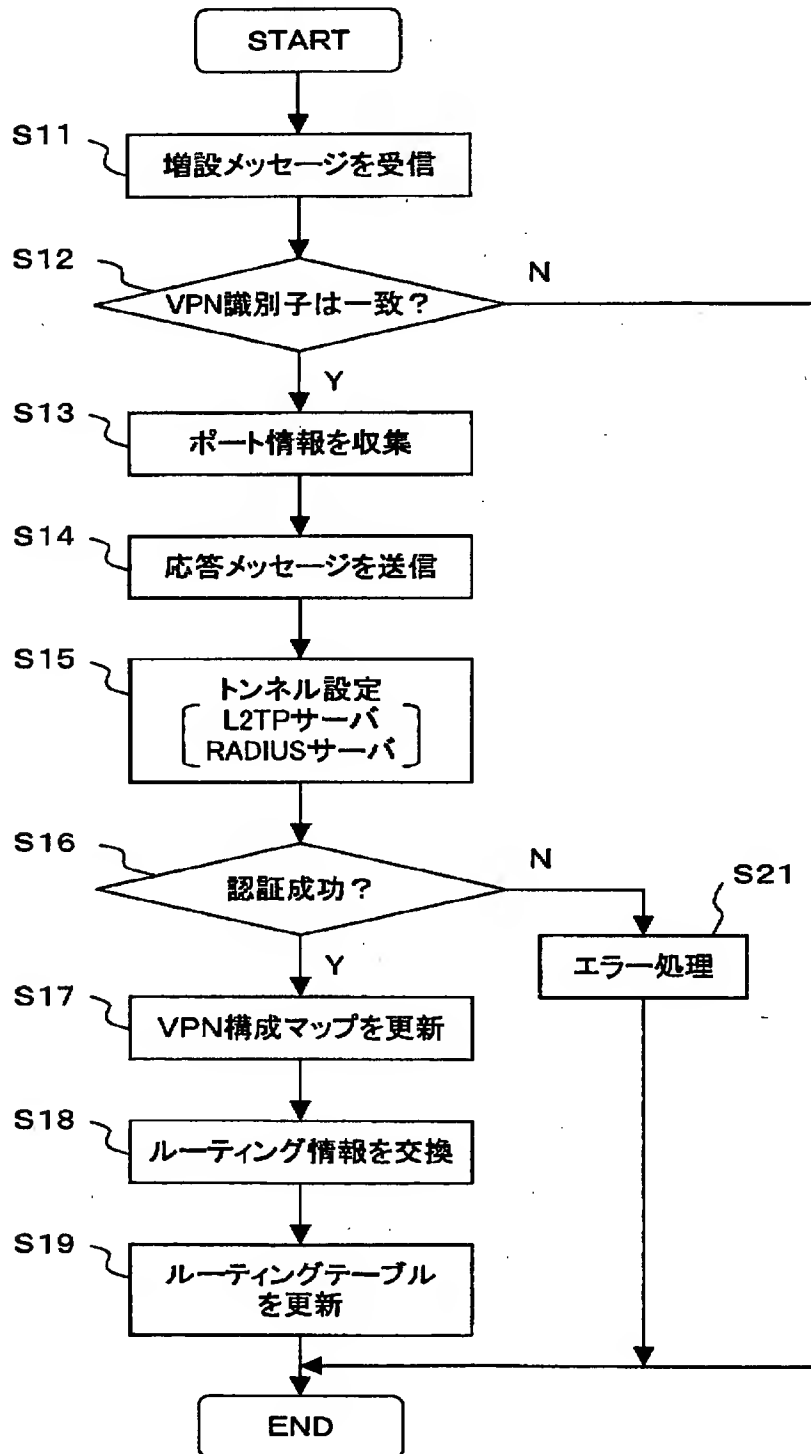
【図 8】

新たに追加されたVRポートにおいてルーティングテーブルを作成する処理のフローチャート



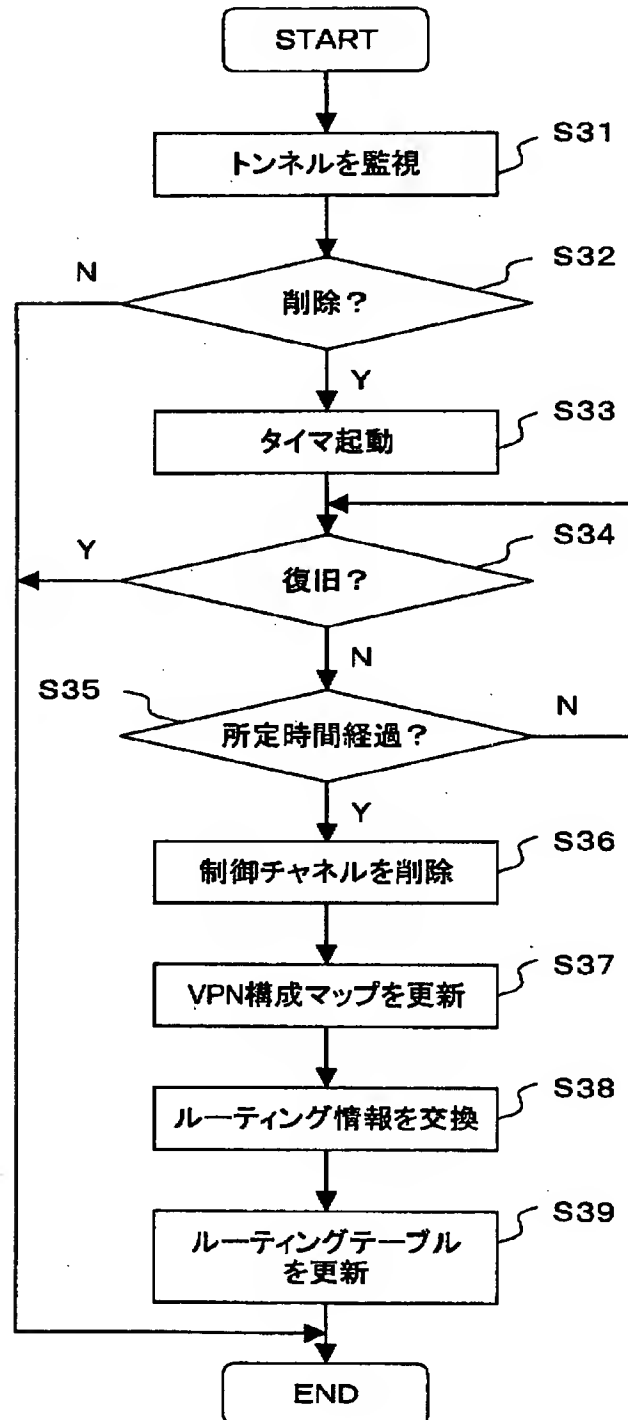
【図9】

新たなVRポートが追加されたときの既設のVRポートの
動作を説明するフローチャート



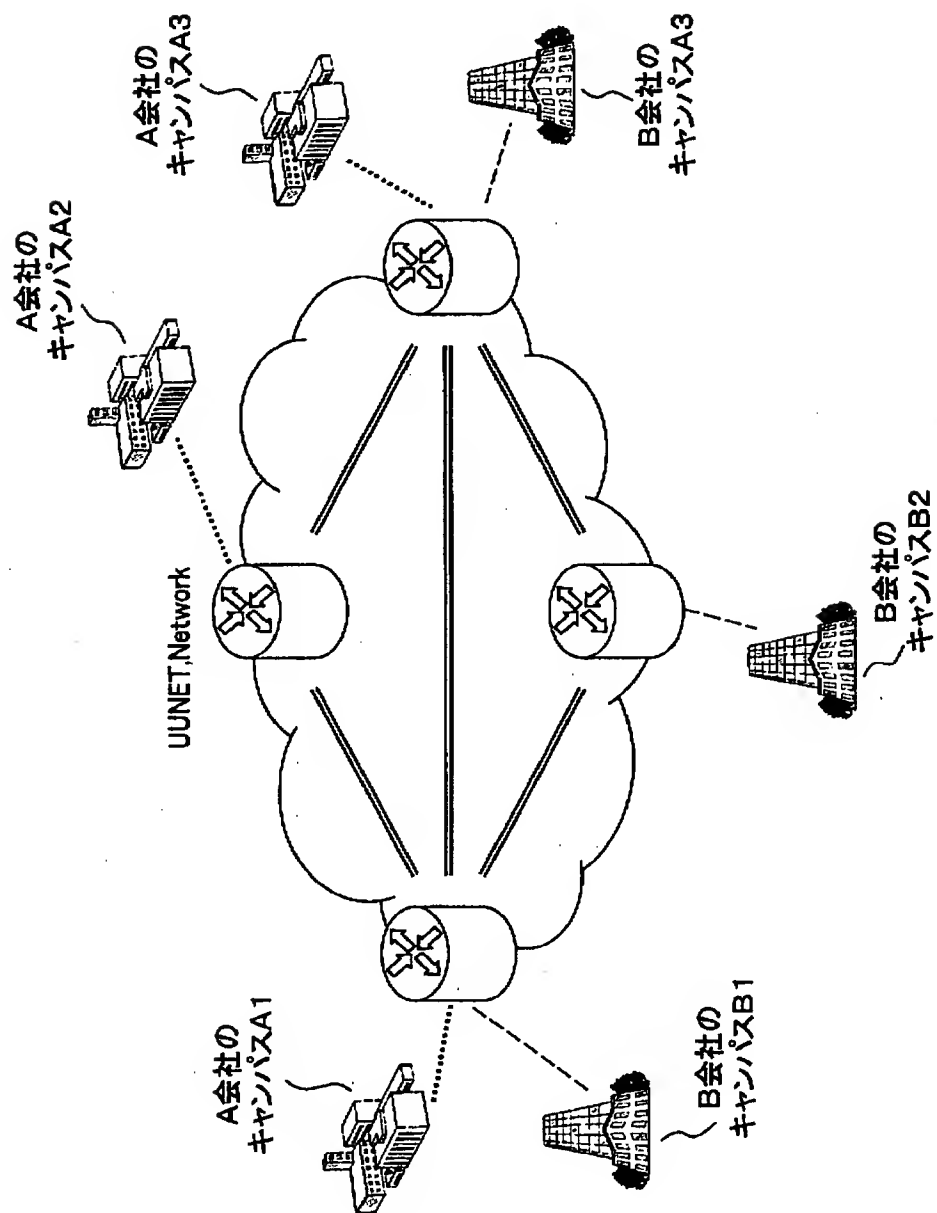
【図10】

あるVRポートが削除されたときに残された
VRポートの処理を示すフローチャート



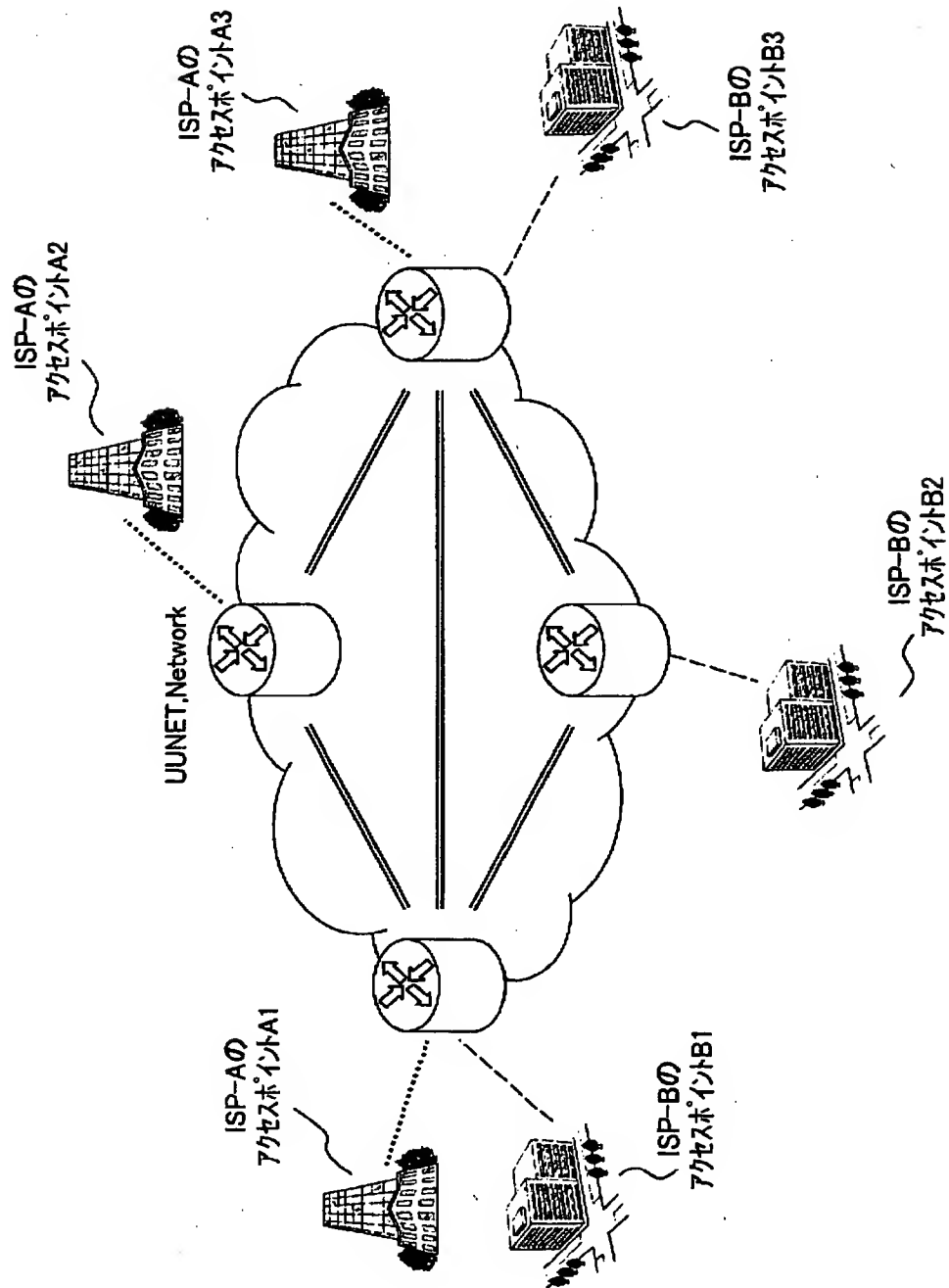
【図 11】

仮想私設網の構築例(その1)



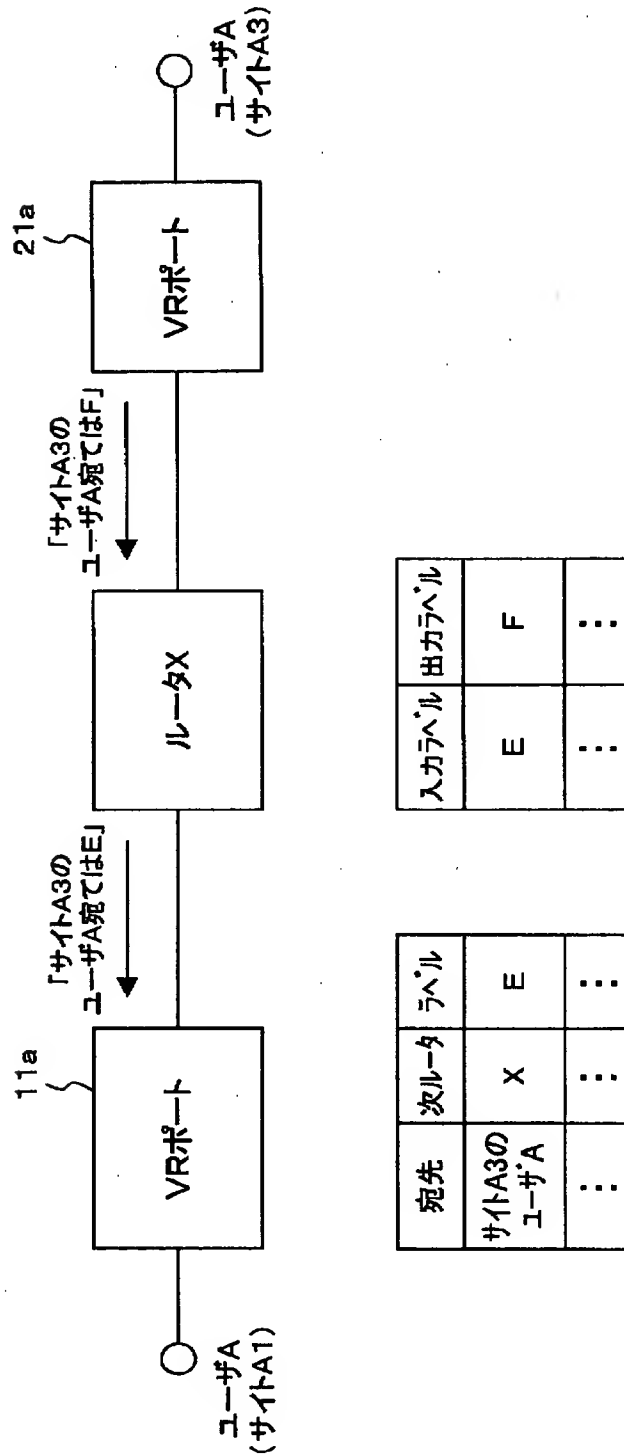
【図 12】

仮想私設網の構築例(その2)



【図 13】

VRポート間でラベルパスを設定する手順の例



【書類名】 要約書

【要約】

【課題】 I P 網を利用した仮想私設網のセキュリティを向上させる。

【解決手段】 ルータ装置は、仮想私設網サービスのユーザ毎に V R ポート 3 0 を備える。各 V R ポート 3 0 は、それぞれ対応する仮想私設網のためのルーティングテーブル 3 2 を有している。制御チャネル終端部 3 3 および V P N 構成モジュール 3 5 は、同一の仮想私設網に属する V R ポートとの間に L 2 T P トンネルを設定する。ゲートウェイプロトコルデーモン 3 1 は、設定された L 2 T P トンネルを介してルーティング情報を交換し、ルーティングテーブル 3 2 を作成／更新する。入力されたパケットは、ルーティングテーブル 3 2 に従ってルーティングされる。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000005223]

| | |
|----------|-----------------------|
| 1. 変更年月日 | 1996年 3月26日 |
| [変更理由] | 住所変更 |
| 住 所 | 神奈川県川崎市中原区上小田中4丁目1番1号 |
| 氏 名 | 富士通株式会社 |